Splunk

Exam Questions SPLK-1001

Splunk Core Certified User Exam

NEW QUESTION 1
When looking at a dashboard panel that is based on a report, which of the following is true?

A. You can modify the search string in the panel, and you can change and configure the visualization.
B. You can modify the search string in the panel, but you cannot change and configure the visualization.
C. You cannot modify the search string in the panel, but you can change and configure the visualization.
D. You cannot modify the search string in the panel, and you cannot change and configure the visualization.

Answer: C

NEW QUESTION 2
What is a primary function of a scheduled report?

A. Auto-detect changes in performance.
B. Auto-generated PDF reports of overall data trends.
C. Regularly scheduled archiving to keep disk space use low.
D. Triggering an alert in your Splunk instance when certain conditions are met.

Answer: D

NEW QUESTION 3
After running a search, what effect does clicking and dragging across the timeline have?

A. Executes a new search.
B. Filters current search results.
C. Moves to past or future events.
D. Expands the time range of the search.

Answer: C

NEW QUESTION 4
What does the values function of the stats command do?

A. Lists all values of a given field.
B. Lists unique values of a given field.
C. Returns a count of unique values for a given field.
D. Returns the number of events that match the search.

Answer: C

NEW QUESTION 5
Which statement is true about Splunk alerts?

A. Alerts are based on searches that are either run on a scheduled interval or in real-time.
B. Alerts are based on searches and when triggered will only send an email notification.
C. Alerts are based on searches and require cron to run on scheduled interval.
D. Alerts are based on searches that are run exclusively as real-time.

Answer: A

NEW QUESTION 6
What is the purpose of using a by clause with the stats command?

A. To group the results by one or more fields.
B. To compute numerical statistics on each field.
C. To specify how the values in a list are delimited.
D. To partition the input data based on the split-by fields.

Answer: A

NEW QUESTION 7
How do you add or remove fields from search results?

A. Use field +to add and field -to remove.
B. Use table +to add and table -to remove.
C. Use fields +to add and fields –to remove.
D. Use fields Plus to add and fields Minus to remove.

Answer: C

NEW QUESTION 8
Which of the following is the most efficient filter for running searches in Splunk?

A. Time
B. Fast mode
C. Sourcetype
D. Selected Fields

Answer: C

NEW QUESTION 9
Which of the following is a best practice when writing a search string?

A. Include all formatting commands before any search terms.
B. Include at least one function as this is a search requirement.
C. Include the search terms at the beginning of the search string.
D. Avoid using formatting clauses, as they add too much overhead.

Answer: D

NEW QUESTION 10
What can be included in the All Fields option in the sidebar?

A. Dashboards
B. Metadata only
C. Non-interesting fields
D. Field descriptions

Answer: D

NEW QUESTION 10
When viewing the results of a search, what is an Interesting Field?

A. A field that appears in any event.
B. A field that appears in every event.
C. A field that appears in the top 10 events.
D. A field that appears in at least 20% of the events.

Answer: D

NEW QUESTION 12
Which is primary function of the timeline located under the search bar?

A. To differentiate between structured and unstructured events in the data.
B. To sort the events returned by the search command in chronological order.
C. To zoom in and zoom out, although this does not change the scale of the chart.
D. To show peaks and/or valleys in the timeline, which can indicate spikes in activity or downtime.

Answer: D

NEW QUESTION 13
What is the primary use for the rare command?

A. To sort field values in descending order.
B. To return only fields containing five of fewer values.
C. To find the least common values of a field in a dataset.
D. To find the fields with the fewest number of values across a dataset.

Answer: C

NEW QUESTION 17
What happens when a field is added to the Selected Fields list in the fields sidebar?

A. Splunk will re-run the search job in Verbose Mode to prioritize the new Selected Field.
B. Splunk will highlight related fields as a suggestion to add them to the Selected Fields list.
C. Custom selections will replace the Interesting Fields that Splunk populated into the list at search time.
D. The selected field and its corresponding values will appear underneath the events in the search results.

Answer: D

NEW QUESTION 18
Three basic components of Splunk are (Choose three.):

A. Forwarders
B. Deployment Server
C. Indexer
D. Knowledge Objects
E. Index

F. Search Head

Answer: ACF

NEW QUESTION 23
What is Splunk?

A. Splunk is a software platform to search, analyze and visualize the machine-generated data.
B. Database management tool.
C. Security Information and Event Management (SIEM).
D. Cloud based application that help in analyzing logs.

Answer: A

NEW QUESTION 24
Splunk Enterprise is used as a Scalable service in Splunk Cloud.

A. True
B. False

Answer: A

NEW QUESTION 25
Which component of Splunk let us write SPL query to find the required data?

A. Forwarders
B. Indexer
C. Heavy Forwarders
D. Search head

Answer: D

NEW QUESTION 27
Log filtering/parsing can be done from _____.

A. Index Forwarders (IF)
B. Universal Forwarders (UF)
C. Super Forwarder (SF)
D. Heavy Forwarders (HF)

Answer: D

NEW QUESTION 32
Splunk shows data in _____ .

A. ASCII Character order.
B. Reverse chronological order.
C. Alphanumeric order.
D. Chronological order.

Answer: B

NEW QUESTION 37
What result will you get with following search index=test sourcetype="The_Questionnaire_P*" ?

A. the_questionnaire _pedia
B. the_questionnaire pedia
C. the_questionnaire_pedia
D. the_questionnaire Pedia

Answer: C

NEW QUESTION 41
Forward Option gather and forward data to indexers over a receiving port from remote machines.

A. False
B. True

Answer: B

NEW QUESTION 44
Parsing of data can happen both in HF and UF.

A. Yes

B. No

Answer: B

NEW QUESTION 48
Upload option creates inputs.conf

A. Yes
B. No

Answer: B

NEW QUESTION 49
Which of the statements are correct about HF? (Choose three.)

A. Parsing
B. Masking
C. Searching
D. Forwarding

Answer: ABD

NEW QUESTION 51
Where does Licensing meter happen?

A. Indexer
B. Parsing
C. Heavy Forwarder
D. Input

Answer: A

NEW QUESTION 55
Matching search terms are highlighted.

A. Yes
B. No

Answer: A

NEW QUESTION 58
You are able to create new Index in Data Input settings.

A. No
B. Yes

Answer: B

NEW QUESTION 60
Which symbol is used to snap the time?

A. @
B. &
C. *
D. #

Answer: A

NEW QUESTION 65
Keywords are highlighted when you mouse over search results and you can click this search result to (Choose three.):

A. Open new search.
B. Exclude the item from search.
C. None of the above.
D. Add the item to search.

Answer: ABD

NEW QUESTION 68
You can view the search result in following format (Choose three.):

A. Table
B. Raw
C. Pie Chart

D. List

Answer: ABD

NEW QUESTION 72

......